REMARKS

Claims 1-21 are rejected in view of LIU and NEWMAN. Reconsideration of the rejection in view of the following comments is respectfully solicited.

The shortcomings of the prior art are described on pages 3 and 4 of the specification. This discussion of the prior art is particularly noteworthy at this time because it characterizes problems associated with the LIU and NEWMAN references. Page 3, beginning at line 4 states:

> Managing encryption keys for millions of users who can potentially send encrypted email messages is a challenging task. Some existing key management systems operate by enrolling public keys for users with an "identity authority." An identity authority typically operates by verifying the identities of owners of public keys as well as keeping track of revoked public keys.
>
> However, existing systems have a number of shortcomings. The verification process is often cumbersome. It typically involves some type of manual check, such as making a telephone call, taking a fingerprint, or receiving personal information from an owner of a public key. Although such manual checks provide a measure of security, they are time-consuming and can be impractical to perform for a large number of users.
>
> Another shortcoming is that the key revocation process does not work well. Some existing systems make use of a "certificate revocation list" (CRL), which contains a listing of revoked certificates. Before using a public key, a client typically checks a locally stored copy of a CRL to verify that the public key has not been revoked. However, a locally stored copy of a CRL may be updated only occasionally (for example, once a week), which means the locally stored copy of the CRL may not be current. This can create problems. For example, an employee who leaves a company may continue to receive sensitive encrypted email messages until the locally stored copy of the CRL is updated.

> Furthermore, a CRL can grow very large over time as more and more certificates are revoked. In some cases, a CRL can contain millions of entries! Hence a locally stored coy of a CRL can require a large amount of space to store, and can be cumbersome to update.

The LIU reference discloses an "identity authority" of the type discussed above. In LIU, the user, not the server, initiates the removal of a key. Once a user has initiated the process of removing a key, the server generates "a confirmation request", which is sent to the user. See, e.g., column 29, lines 21-40. A "confirmation request" is confirming an action initiated by the user. This stands in sharp contrast to the claimed invention.

The independent claims include a number of limitations that are not shown or suggested by LIU. For example, claim 1 recites "periodically sending a verification request from the server to the client asking if the client public key remains valid". First, observe that the server, not the user, initiates this action. This is in contrast to LIU, where the user initiates the action. Next, observe that the server is sending a "verification request" to test the user's existence. In LIU, the user's existence is known, because the user initiated the request. The "confirmation request" in LIU is not a "verification request". The "confirmation request" in LIU operates to provide the user with a second chance to endorse the user-initiated process of removing a key. Thus, LIU does not show or suggest the claimed server initiated operation. Further, LIU does not show or suggest the use of the claimed verification request.

NEWMAN also fails to show or suggest the limitations of the claimed invention. First, NEWMAN never addresses the issue of removing or deleting key information. NEWMAN only discusses adding new public keys associated with new FAX units being added to the network. Even assuming for the sake of argument that NEWMAN inherently has some type of revocation process, then NEWMAN is merely operating in accordance with a "certificate revocation list" technique. As discussed above, such a prior art approach is problematic. In sum, NEWMAN, at best, teaches a "certificate revocation list" technique that is known in the prior art as a flawed mechanism. The invention overcomes the problems associated with a "certificate revocation

list". In addition, the invention provides a number of advantages that are not shown or suggested by the prior art of record. As stated in the specification on page 15, lines 15-18:

> Note that the above-described process removes public keys belonging to users who lose access to their email account, or users who die. Moreover, the above-described process solves the problem of users not being able to remove their public keys if they forget their password.

The prior art of record does not address these problems in any way. However, the present application discloses and claims a technique to overcome these problems.

In sum, claim 1 includes a number of limitations that are not shown or suggested by the prior art. Thus, claim 1 should be in a condition for allowance. Claims 2-7 are dependent upon claim 1 and therefore should also be in a condition for allowance. Claim 8 includes limitations of the type discussed in connection with claim 1. Thus, claim 8 and its dependent claims 9-14 should also be in a condition for allowance. Similarly, claim 15 includes limitations of the type discussed in connection with claim 1. Thus, claim 15 and its dependent claims 16-21 should also be in a condition for allowance.

If there are any residual prosecution issues that can be resolved with a telephone call, the Patent Examiner is requested to contact the undersigned.

Dated: Oct. 18, 2004

Respectfully submitted,
COOLEY GODWARD LLP

Cooley Godward LLP
ATTN: Patent Group
Five Palo Alto Square
3000 El Camino Real
Palo Alto, CA 94306-2155
Tel: (650) 843-5000
Fax: (650) 857-0663

By: _____
William S. Galliani
Reg. No. 33,885